**PCT** WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04M 15/00, G06F 1/00 — A1

(11) International Publication Number: WO 00/67460

(43) International Publication Date: 9 November 2000 (09.11.00)

(21) International Application Number: PCT/GB00/01676

(22) International Filing Date: 28 April 2000 (28.04.00)

(30) Priority Data:
9910268.3 4 May 1999 (04.05.99) GB

(71) Applicant *(for all designated States except US)*: NORTEL NETWORKS LIMITED [CA/CA]; World Trade Center of Montreal, 8th floor, 380 St Antoine Street West, Montreal, Quebec H2Y 3YF (CA).

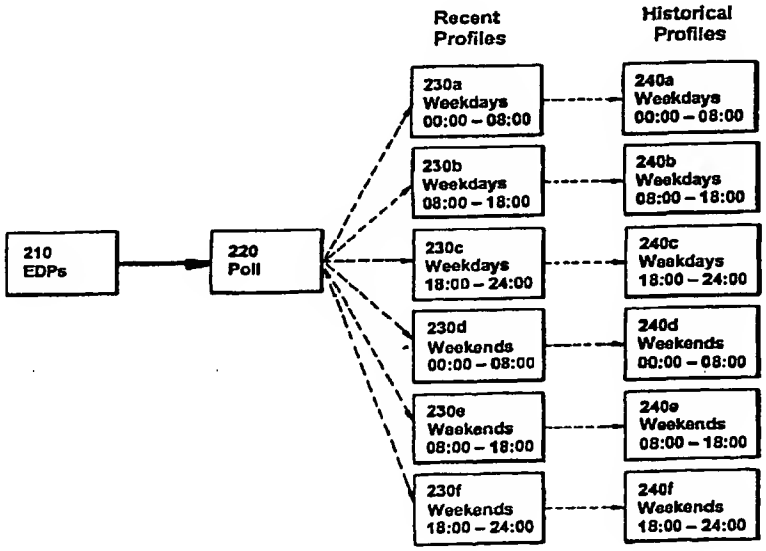
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BUTCHART, Katherine [GB/GB]; 16 Barham Road, Stevenage, Hertfordshire SG2 9HX (GB). DEMPSEY, Derek [GB/GB]; 7 Ulverstone Road, West Norwood, London SE27 0AJ (GB).

(74) Agent: RYAN, John; Nortel Networks Corporation, London Road, Harlow, Essex CM17 9NA (GB).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
*With international search report.*
*Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.*

(54) Title: METHOD AND SYSTEM FOR FRAUD DETECTION IN TELECOMMUNICATIONS




(57) Abstract

A method and apparatus for profiling a flow of event data packets. The method comprises the steps of: receiving data defining sub-periods which partition a base time period, creating a profile of recent behaviour for each sub-period, and allocating each event data packet to one of the sub-periods according to a time indication associated with the event data packet. The method and apparatus may be used in anomaly detection within data streams and, in particular, account fraud detection where the event data relates to account usage.

*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| AL | Albania | ES | Spain | LS | Lesotho | SI | Slovenia |
| AM | Armenia | FI | Finland | LT | Lithuania | SK | Slovakia |
| AT | Austria | FR | France | LU | Luxembourg | SN | Senegal |
| AU | Australia | GA | Gabon | LV | Latvia | SZ | Swaziland |
| AZ | Azerbaijan | GB | United Kingdom | MC | Monaco | TD | Chad |
| BA | Bosnia and Herzegovina | GE | Georgia | MD | Republic of Moldova | TG | Togo |
| BB | Barbados | GH | Ghana | MG | Madagascar | TJ | Tajikistan |
| BE | Belgium | GN | Guinea | MK | The former Yugoslav Republic of Macedonia | TM | Turkmenistan |
| BF | Burkina Faso | GR | Greece | | | TR | Turkey |
| BG | Bulgaria | HU | Hungary | ML | Mali | TT | Trinidad and Tobago |
| BJ | Benin | IE | Ireland | MN | Mongolia | UA | Ukraine |
| BR | Brazil | IL | Israel | MR | Mauritania | UG | Uganda |
| BY | Belarus | IS | Iceland | MW | Malawi | US | United States of America |
| CA | Canada | IT | Italy | MX | Mexico | UZ | Uzbekistan |
| CF | Central African Republic | JP | Japan | NE | Niger | VN | Viet Nam |
| CG | Congo | KE | Kenya | NL | Netherlands | YU | Yugoslavia |
| CH | Switzerland | KG | Kyrgyzstan | NO | Norway | ZW | Zimbabwe |
| CI | Côte d'Ivoire | KP | Democratic People's Republic of Korea | NZ | New Zealand | | |
| CM | Cameroon | | | PL | Poland | | |
| CN | China | KR | Republic of Korea | PT | Portugal | | |
| CU | Cuba | KZ | Kazakstan | RO | Romania | | |
| CZ | Czech Republic | LC | Saint Lucia | RU | Russian Federation | | |
| DE | Germany | LI | Liechtenstein | SD | Sudan | | |
| DK | Denmark | LK | Sri Lanka | SE | Sweden | | |
| EE | Estonia | LR | Liberia | SG | Singapore | | |

# METHOD AND SYSTEM FOR FRAUD DETECTION IN TELECOMMUNICATIONS

## FIELD OF THE INVENTION

The present invention relates to a method and apparatus for performing pattern recognition within event streams, and a system incorporating the same.

## BACKGROUND TO THE INVENTION

In recent years there has been a rapid increase in the number of commercially operated telecommunications networks in general and in particular wireless telecommunication networks. Associated with this proliferation of networks is a rise in fraudulent use of such networks the fraud typically taking the form of gaining illicit access to the network, and then using the network in such a way that the fraudulent user hopes subsequently to avoid paying for the resources used. This may for example involve misuse of a third party's account on the network so that the perpetrated fraud becomes apparent only when the third party is charged for resources which he did not use.

Since fraudulent use of a single account can cost a network operator a large sum of money within a short space of time it is important that the operator be able to identify and deal with the most costly forms of fraud at the earliest possible time.

One of the steps employed in, but not limited to use in, such fraud detection systems is pattern recognition from event streams.

Pattern recognition for event streams can be achieved by building up profiles of the behaviour of an entity and performing pattern recognition over these profiles. In order for an entity to be profiled in this way, the entity must be able to have events associated with it. Examples of entities are: a single subscriber in a telephone network, a user accessing a data network, a switch in a telephone network or a server in a data network. The events to be associated with the user must be able to be represented in an Event Data Packet (EDP). The profiles of entities behaviour are

compared with known patterns of unacceptable behaviour to determine if the system should alert the end user to the entities behaviour pattern.

The flow of Event Data Packets 110 of information through a profiling pattern recognition system is shown in Figure 1. The Recent profile 130 represents the typical usage for the entity over a recent period of time, approximately the last week. The Historical profile 140 represents the typical use for the entity over a preceding and longer time period, for example approximately the last six weeks. The EDPs are all accumulated into Polls of information. A Poll 120 is a set of EDPs received over a particular time period (e.g. 4 hours). The Poll information is then used to update the values in the Recent profile, and the Recent profile is then used to update the values in the Historical profile. The solid arrow between the EDPs and the Poll indicates that the information in each Poll is directly created from the EDPs. The dotted arrow between the Poll and the Recent indicates that the Poll information is used only to update the Recent behaviour, as is true for the Recent to Historical.

In an example where the EDPs are Call Detail Records (CDRs) and the profiles represent voice telephony usage is given the profiles may consist of number of calls made and the duration of national and international calls. Table 1 shows an example of Recent and Historical profiles for such an example.

| Period | Calls | National Duration (sec) | International Duration (sec) |
|---|---|---|---|
| **Recent Profile** | 2.5 | 300 | 200 |
| **Historic Profile** | 2.0 | 250 | 200 |

**Table 1: Voice telephony recent and historic profile example**

If subsequent CDRs create a Poll of:

- calls 3,
- national 500,
- international 100.

Then after polling and once all updates to Recent and Historic profiles have completed the Recent and Historic profiles may be as shown in Table 2.

The new recent profile is derived from the previous recent profile plus a proportion of the difference between the new and old recent profiles

The new historic profile is derived from the previous historic profile plus a proportion of the difference between the new and old historic profiles, but the proportions typically differ from that of the recent profile case in that a higher proportion of the old historic profile is taken.

| Period | Calls | National Duration (s) | International Duration (s) |
|---|---|---|---|
| Recent Profile | 2.75 | 280 | 175 |
| Historic Profile | 2.1 | 255 | 195 |

**Table 2: Voice telephony recent and historic profile example after update**

It can be seen that the Recent profile has moved towards the newly added Poll profile and the Historic toward the previous Recent profile. These profiles provide a view of the entity's behaviour and how it changes over time. The profiles of behaviour can then be used for pattern recognition to identify which entity's behaviour reflects patterns to which the user of system wishes to be alerted.

There are however the following limitations to the method described above:

The Recent and Historic profiles are built up from a series of Poll profiles. In order for the Recent and Historic profiles to maintain their integrity all Poll profiles must cover the same amount of time, for example a 4 hour period.

The period of time the Polls must all cover must not be too small, otherwise natural variations in behaviour will appear to be anomalous. A typical recommended minimum is two hours.

These two limitations, taken in consideration, mean that this method cannot be used for real time data feeds.

It is also incumbent upon the user to ensure that the data given to the product is split into appropriately sized chunks. This can be a burden to the user if, for example, hardware downtime means it is necessary to feed a backlog of data into the system.

The profiles generated only represent the active periods for the user, this means that a user who is active in only one two hour period a week could have a similar profile to a user who is active in twenty of the two hour periods in a week.

The nature of the data in the profile – as an average of activity in all X minute periods where the user had actually been active – where X is the duration of the Poll, is not intuitive to many end users of the system.

In order for pattern recognition to occur effectively, the known patterns have to be represented in the same time period that the systems polls over. This can increase training times for the account fraud detection system which analyses the Poll, Recent profile, and Historical profile information in order to identify anomalies.

## OBJECT OF THE INVENTION

The invention seeks to provide an improved method and apparatus for behavioural pattern recognition for event streams in general and for event streams in an account fraud detection systems in particular.

## SUMMARY OF THE INVENTION

According to a first aspect of the present invention there is provided a method of profiling a flow of event data packets comprising the steps of: receiving data defining a plurality of sub-periods which partition a base time period; creating a profile of recent behaviour for each of said sub-periods; allocating each Event Data Packet to one of said sub-periods according to a time indication associated with said Event Data Packet.

The method may also comprise the steps of: creating a profile of historical behaviour for each of said sub-periods; at the end of said Base Time Period updating each of said Historical profiles responsive to the previous value of said Historical profile and a corresponding Recent profile, and resetting each said Recent profile.

The method may also comprise the steps of: calculating an Event density for at least one of said Recent profiles.

In a preferred embodiment, the said step of calculating an Event density comprises the steps of: identifying a current time; identifying a Recent profile within which said current time falls; dividing a number of events recorded in said Recent profile by a time duration determined by a difference between said current time and a start time of sub-period associated with said Recent profile.

Said Event Data may correspond to time intervals of differing length.

The method may be used to capture a representation of inactivity within said flow.

The method may also be used to permit trend analysis for an initial sub-period during said sub-period.

According to a further aspect of the present invention there is provided a method of performing anomaly detection on a stream of Event Data Packets and comprising the steps of: receiving data defining a plurality of sub-periods which partition a base time period; creating a Recent profile for each of said sub-periods; allocating each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

According to a further aspect of the present invention there is provided a method of account fraud detection comprising the steps of: receiving data defining a plurality of sub-periods which partition a base time period; creating a Recent profile for each of said sub-periods; receiving a series of Event Data Packets relating to account use; allocating each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

In a preferred embodiment account use relates to telecommunications network use.

In a preferred embodiment said Event Data Packets are call detail records.

According to a further aspect of the present invention there is provided a method of network intrusion detection comprising the steps of: receiving data defining a plurality of sub-periods which partition a base time period; creating a Recent profile for each of said sub-periods; receiving a series of Event Data Packets relating to account use; allocating each said Event Data Packet to a sub-period according to a time indication in said Event Data Packet.

In a preferred embodiment said Event Data Packets relate to network audit log data.

In a preferred embodiment said Event Data Packets relate to IP packet data.

According to a further aspect of the present invention there is provided a system for profiling a flow of event data packets comprising: apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period; apparatus arranged to create and store a Recent profile for each of said sub-periods; allocating each Event Data Packet to one of said sub-periods according to a time indication associated with said Event Data Packet.

The system may be arranged to receive a plurality of flows and to perform processing on each flow independently of each other.

According to a further aspect of the present invention there is provided a system for performing anomaly detection on a stream of Event Data

Packets and comprising: apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period; apparatus arranged to create a profile of recent behaviour for each of said sub-periods; apparatus arranged to allocate each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

According to a further aspect of the present invention there is provided a system for account fraud detection comprising: apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period; apparatus arranged to create a profile of recent behaviour for each of said sub-periods; apparatus arranged to allocate each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

According to a further aspect of the present invention there is provided a system for network intrusion detection comprising: apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period; apparatus arranged to create a profile of recent behaviour for each of said sub-periods; apparatus arranged to allocate each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

The invention also provides for a system for the purposes profiling a flow of event data packets which comprises one or more instances of apparatus embodying the present invention, together with other additional apparatus.

According to a further aspect of the present invention there is provided software on a machine readable medium arranged for profiling a flow of event data packets by: receiving data defining a plurality of sub-periods which partition a base time period; creating a Recent profile for each of said sub-periods; allocating each Event Data Packet to one of said sub-periods according to a time indication associated with said Event Data Packet.

The preferred features may be combined as appropriate, as would be apparent to a skilled person, and may be combined with any of the aspects of the invention.

## BRIEF DESCRIPTION OF THE DRAWINGS

In order to show how the invention may be carried into effect, embodiments of the invention are now described below by way of example only and with reference to the accompanying figures in which:

Figure 1 shows a block diagram of information flow in a behavioural pattern recognition system in accordance with the prior art;

Figure 2 shows a block diagram of information flow in a behavioural pattern recognition system in accordance with the present invention.

## DETAILED DESCRIPTION OF INVENTION

The method proposed here is illustrated in Figure 2. The EDPs 210 (in this example taking the form of Call Detail Records (CDRs)) again feed into a Poll 220 of information and the Poll information is used to update the values in the Recent profiles 230a-f In this case each entity has associated with it multiple Recent Profiles (six are shown but more or fewer may be used), where each Recent profile represents a period of time within a week (though a larger or shorter base period could be used), for example Saturday and Sunday between midnight and 8am. The Recent Profiles together cover the whole of a week period. Each Recent Profile has a related Historic Profile 240a-f which covers the same time period.

Recent Profiles are filled until they contain all the data for the time period they cover. Once filled the values are used to update the corresponding Historic profile, and then the Recent profile values are reset to zero, and filled with the next CDRs in the time covered by the profile.

For example, a customer of voice telephony may have the Recent profiles of behaviour illustrated in Table 3 and corresponding Historic profiles illustrated in Table 4.

| Profile Number | Period | Calls | National Duration (s) | International Duration (s) |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1 | Weekdays, 0:00 – 08:00 | 1 | 25 | 0 |
| 2 | Weekdays, 08:00 – 18:00 | 10 | 500 | 400 |
| 3 | Weekdays, 18:00 – 24:00 | 0 | 0 | 0 |
| 4 | Weekends, 0:00 – 08:00 | 0 | 0 | 0 |
| 5 | Weekends, 08:00 – 18:00 | 5 | 255 | 15 |
| 6 | Weekends, 18:00 – 24:00 | 0 | 0 | 0 |

**Table 3: Voice telephony recent profiles example**

| Profile Number | Period | Calls | National Duration (s) | International Duration (s) |
|---|---|---|---|---|
| 1 | Weekdays, 0:00 – 08:00 | 1.5 | 30 | 2 |
| 2 | Weekdays, 08:00 – 18:00 | 8.5 | 800 | 250 |
| 3 | Weekdays, 18:00 – 24:00 | 2 | 25 | 15 |
| 4 | Weekends, 0:00 – 08:00 | 0 | 0 | 0 |
| 5 | Weekends, 08:00 – 18:00 | 2 | 25 | 19 |
| 6 | Weekends, | 0 | 0 | 0 |

| | | | | |
|---|---|---|---|---|
| | 18:00 – 24:00 | | | |

**Table 4: Voice telephony historic profiles example**

A collection of Event Data (CDRs) is then presented to the system. The CDRs cover 7am on a Monday through to 1pm on the same Monday. The previous collection of data presented to the system had contained a CDR for 5am on the same Monday.

The CDR at 7am is added to Recent Profile 1. When this profile is 'complete' the historic profile is updated. When the next time period is entered its recent profile values are reset to zero and new values accumulated.

The Recent and Historical profiles after the data has been processed areas illustrated in Tables 5 and 6 respectively.

| Profile Number | Period | Calls | National Duration (s) | International Duration (s) |
|---|---|---|---|---|
| 1 | Weekdays, 0:00 – 08:00 | 2 | 355 | 0 |
| 2 | Weekdays, 08:00 – 18:00 | 4 | 300 | 425 |
| 3 | Weekdays, 18:00 – 24:00 | 0 | 0 | 0 |
| 4 | Weekends, 0:00 – 08:00 | 0 | 0 | 0 |
| 5 | Weekends, 08:00 – 18:00 | 5 | 255 | 15 |
| 6 | Weekends, 18:00 – 24:00 | 0 | 0 | 0 |

**Table 5: Voice telephony recent profiles after processing**

| Profile Number | Period | Calls | National Duration (s) | International Duration (s) |
|---|---|---|---|---|
| 1 | Weekdays, 0:00 – 08:00 | 2.0 | 62.5 | 1.8 |
| 2 | Weekdays, 08:00 – 18:00 | 8.05 | 750 | 267.5 |
| 3 | Weekdays, 18:00 – 24:00 | 2 | 25 | 15 |
| 4 | Weekends, 0:00 – 08:00 | 0 | 0 | 0 |
| 5 | Weekends, 08:00 – 18:00 | 2 | 25 | 19 |
| 6 | Weekends, 18:00 – 24:00 | 0 | 0 | 0 |

**Table 6: Voice telephony historic profiles after processing**

The only Recent profiles changed are those that cover the same time period as the CDRs in the poll namely periods 1 and 2. The only Historic profile changed is in period 1, the values in the Recent profile having been used to update the Historic profile. After updating the Historic profile, the Recent profile is then reset to zero before new CDR information is added to it.

Historic profiles are only updated once the Recent profile has been filled with all the information for that time period. This means that the size of the Poll has no influence over the Historic profiles, and the Recent profiles can contain details for any sub-period of the time period they cover, or the whole time period.

The profiles of behaviour are converted into Event Densities before pattern recognition is performed on them. Event Densities are produced by dividing the event data value by the number of seconds in the period during which those events occurred. For example, Table 6 shows an example set of Historic profile values and the corresponding event densities values where the period covered 14400 seconds (4 hours).

| Period | Calls | National Duration | International Duration |
|---|---|---|---|
| **Historic Profile Values** | 10 | 200 s | 300 s |
| **Event Densities** | 10 / 14400 (= 0.00069) | 200 / 14400 (= 0.00139) | 300 / 14400 (= 0.02083) |

**Table 7: Voice telephony historic profiles after processing**

Event densities for historic profiles provide an average of behaviour over the whole time period. This means that dividing by the number of seconds in the time period gives the normal amount of behaviour in any one second. These are generally small values.

Recent profiles however may or may not contain values for the whole the time period they cover. Frequently the Recent profile that is being analysed is not yet complete. For example, if ten minutes of event data require analysing for the time period 9.15am to 9.25am then a recent profile that covers the time period 8am to 6pm will be updated, but the time period for this profile is not yet complete. As the period is incomplete the number of seconds to divide by is calculated as follows. The complete time period is divided into blocks of time, for example 30 minutes. A usage period consists of x of these blocks of time. The event data in the current incomplete Recent profile is divided by the number of seconds in the blocks covered so far. So event data covering up to 9.25 am has covered three 30 minute blocks so far and the values are divided by 5400 seconds (90 minutes). Conversion into densities enables pattern recognition to be performed over event data that covers just a portion of the total time period.

This method has the advantages that:

- the polls of event data can be of any size whilst still allowing the profiles produced by the system to maintain their integrity;
- polls of data for very small time periods can be handled easily;
- the preceding two advantages have the consequence that the system is suitable for both real time feeds and bulk batch feeds of poll data;
- there is consequently no burden on the end user to divide up the event data into fixed sized chunks; and
- the profiles represent accurately the behaviour of the user, including a representative of inactivity by the user, and a representation of the time of use.

This method may be used in several application areas. These include telephony fraud detection using call detail records (CDRs), anomaly detection on data streams, network intrusion detection using audit log data or IP packet data. The method also provides a means of comparison between recent behaviour and past behaviour for event streams that has potentially wide application for the rapid detection of behavioural changes.

Any range or device value given herein may be extended or altered without losing the effect sought, as will be apparent to the skilled person for an understanding of the teachings herein.

**CLAIMS**

1. A method of profiling a flow of event data packets comprising the steps of:

receiving data defining a plurality of sub-periods which partition a base time period;

creating a profile of recent behaviour for each of said sub-periods;

allocating each Event Data Packet received to one of said sub-periods according to a time indication associated with said Event Data Packet.

2. A method according to claim 1 comprising the steps of:

creating a profile of historical behaviour for each of said sub-periods;

at the end of said Base Time Period updating each of said Historical profiles responsive to the previous value of said Historical profile and a corresponding Recent profile, and resetting each said Recent profile.

3. A method according to any one of claims 1 - 2 additionally comprising the step of:

calculating an Event density for at least one of said Recent profiles.

4. A method according to claim 3 wherein said step of calculating an Event density comprises the steps of:

identifying a current time;

identifying a Recent profile within which said current time falls;

dividing a number of events recorded in said Recent profile by a time duration determined by a difference between said current time and a start time of sub-period associated with said Recent profile.

5. A method according to any one of claims 1 - 4, wherein said Event Data may correspond to time intervals of differing length.

6. A method according to any one of claims 1 - 5, whereby to capture a representation of inactivity within said flow.

7. A method according to any one of claims 1 - 6, whereby to permit trend analysis for an initial sub-period during said sub-period.

8. A method of performing anomaly detection on a stream of Event Data Packets and comprising the steps of:

receiving data defining a plurality of sub-periods which partition a base time period;

creating a Recent profile for each of said sub-periods;

allocating each Event Data Packet to a sub-period according to a time indication in said Event Data Packet.

9. A method of account fraud detection comprising the steps of:

receiving data defining a plurality of sub-periods which partition a base time period;

creating a Recent profile for each of said sub-periods;

receiving a series of Event Data Packets relating to account use;

allocating each Event Data Packet to a sub-period according to a time indication in said Event Data Packet.

10. A method of account fraud detection according to claim 9, wherein said account use relates to telecommunications network use.

11. A method of account fraud detection according to any one of claims 9 - 10, wherein said Event Data Packets are call detail records.

12. A method of network intrusion detection comprising the steps of:

receiving data defining a plurality of sub-periods which partition a base time period;

creating a Recent profile for each of said sub-periods;

receiving a series of Event Data Packets relating to account use;

allocating each said Event Data Packet to a sub-period according to a time indication in said Event Data Packet.

13. A method of network intrusion detection according to claim 12, wherein said Event Data Packets relate to network audit log data.

14. A method of network intrusion detection according to claim 12, wherein said Event Data Packets relate to IP packet data.

15. A system for profiling a flow of event data packet polls comprising:

apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period;

apparatus arranged to create and store a Recent profile for each of said sub-periods;

allocating each Event Data Packet in said Poll to one of said sub-periods according to a time indication associated with said Event Data Packet.

16. A system according to claim 15 arranged to receive a plurality of flows and to perform process each flow independently of each other.

17. A system for performing anomaly detection on a stream of Event Data Packets and comprising:

apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period;

apparatus arranged to create a Recent profile for each of said sub-periods;

apparatus arranged to allocate each Event Data Packet to a sub-period according to a time indication in said Event Data Packet.

18. A system for account fraud detection comprising:

apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period;

apparatus arranged to create a profile of recent behaviour for each of said sub-periods;

apparatus arranged to allocate each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

19. A system for of network intrusion detection comprising:

apparatus arranged to receive and store data defining a plurality of sub-periods which partition a base time period;

apparatus arranged to create a profile of recent behaviour for each of said sub-periods;

apparatus arranged to allocate each Event Data Packet to a sub-period according a time indication in said Event Data Packet.

20. Software on a machine readable medium arranged for profiling a flow of event data packet polls by:

receiving data defining a plurality of sub-periods which partition a base time period;

creating a profile of recent behaviour for each of said sub-periods;

allocating each Event Data Packet inset Poll to one of said sub-periods according to a time indication associated with said Event Data Packet.

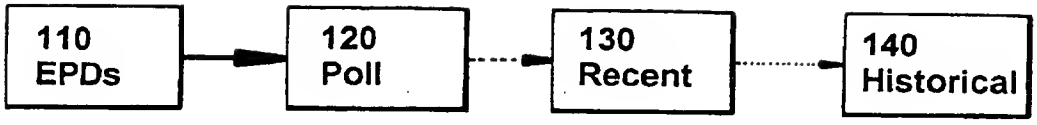



*Fig. 1*

2/2

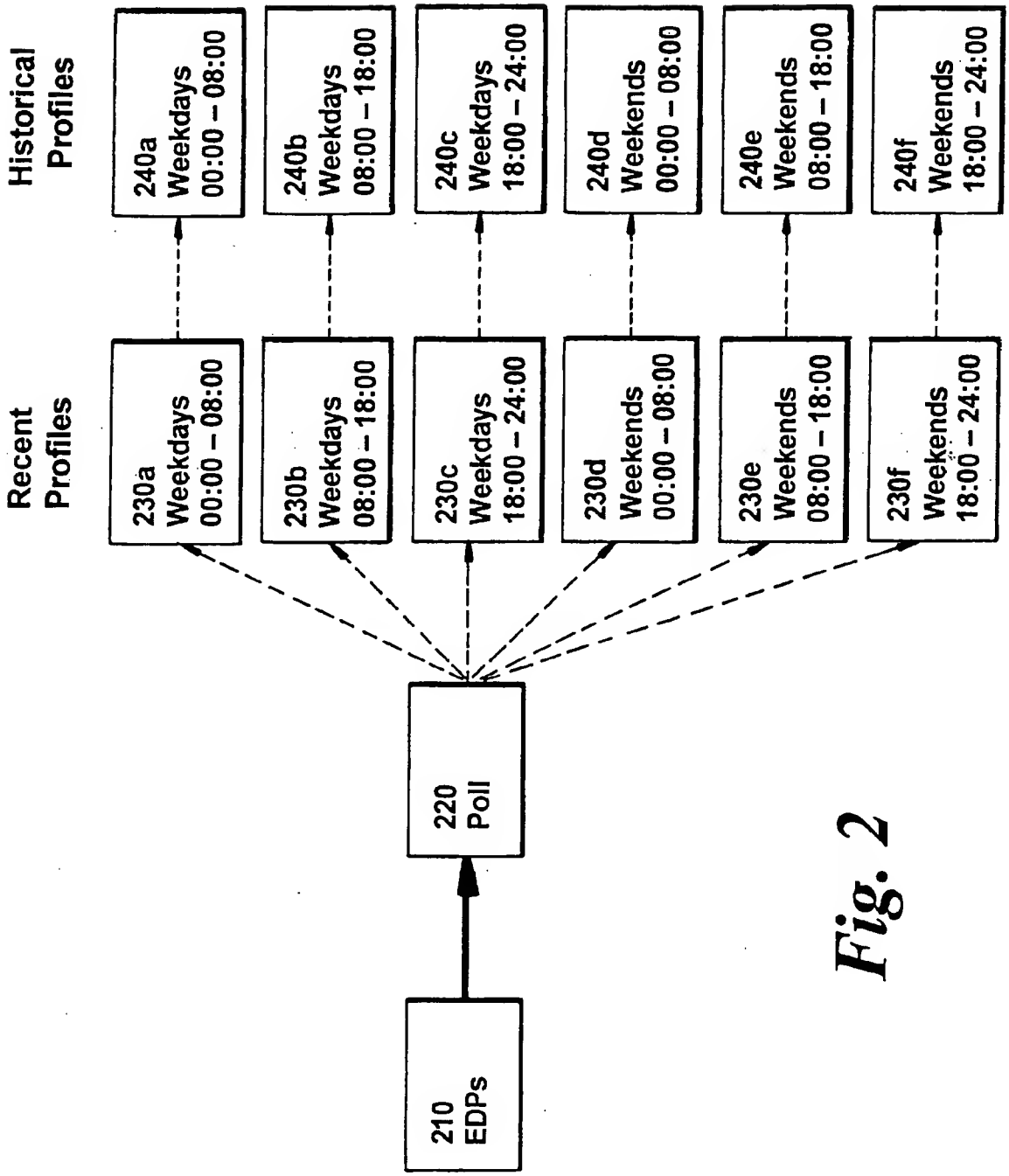

Historical Profiles
240a Weekdays 00:00 – 08:00
240b Weekdays 08:00 – 18:00
240c Weekdays 18:00 – 24:00
240d Weekends 00:00 – 08:00
240e Weekends 08:00 – 18:00
240f Weekends 18:00 – 24:00
Recent Profiles
230a Weekdays 00:00 – 08:00
230b Weekdays 08:00 – 18:00
230c Weekdays 18:00 – 24:00
230d Weekends 00:00 – 08:00
230e Weekends 08:00 – 18:00
230f Weekends 18:00 – 24:00
220 Poll
210 EDPs

*Fig. 2*

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/01676

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04M15/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04M G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 97 03533 A (NORTHERN TELECOM LTD ;BARSON PAUL COLIN (GB); MCASKI GILL (GB); HO) 30 January 1997 (1997-01-30) | 9-11,18 |
| Y | page 2, line 26 -page 3, line 35 | 12,13,19 |
| A | page 5, line 1 -page 8, line 2 | 14 |
| Y | BURGE P ET AL: "Fraud detection and management in mobile telecommunications networks" EUROPEAN CONFERENCE ON SECURITY AND DETECTION, 28 April 1997 (1997-04-28), XP002085420 page 93, column 1, line 24 -page 95, column 2, line 7 | 12,13,19 |

-/—

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 28 August 2000 | 20. 09. 2000 |
| Name and mailing address of the ISA<br>Europaan Patant Office, P.B. 5816 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,<br>Fax: (+31–70) 340–3016 | Authorized officer<br>Schweitz, M |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 00/01676

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication,where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | WO 96 31043 A (GIBBINGS CHRISTOPHER JOHN ;PEEL STEPHEN JOHN (GB); REGNAULT JOHN C) 3 October 1996 (1996-10-03) page 1, line 1 -page 6, line 29 | 9-14,18, 19 |
| A | WO 99 05844 A (BRITISH TELECOMM ;EDWARDS ALEXANDER FRASER MILES (GB)) 4 February 1999 (1999-02-04) page 8, line 6 -page 9, line 21 | 9-14,18, 19 |
| A | BARSON P ET AL: "The detection of fraud in mobile phone networks" INTERNATIONAL NEURAL NETWORK SOCIETY ANNUAL MEETING. PROCEEDINGS OF WORLD CONGRESS ON NEURAL NETWORKS,XX,XX, vol. 6, no. 4, 16 April 1996 (1996-04-16), pages 477-484, XP002085421 the whole document | 9-14,18, 19 |
| A | US 5 375 244 A (MCNAIR BRUCE E) 20 December 1994 (1994-12-20) abstract | 9-14,18, 19 |

2

# INTERNATIONAL SEARCH REPORT

...ernational application No.
PCT/GB 00/01676

**Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)**

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 1-8, 15-17, 20
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the peyment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 1-8, 15-17, 20

Present claims 1-8, 15-17 and 20 relate to an extremely large number of possible methods, systems and products. The only fields of application which have been clearly defined in the description of the application are account fraud detection and network intrusion detection. However, the subject-matter of the above mentioned claims could be applied to an unknown number of fields of technology. Thereby, support within the meaning of Article 6 PCT and disclosure within the meaning of Article 5 PCT is to be found for only a very small proportion of the methods, systems and products claimed. In the present case, the claims so lack support, and the application so lacks disclosure, that a meaningful search over the whole of the claimed scope is impossible. Consequently, the search has been carried out for those parts of the claims which appear to be supported and disclosed, namely those parts of the application relating to claims 9-14, 18 and 19.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 00/01676

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9703533 A | 30-01-1997 | GB 2303275 A | 12-02-1997 |
| | | CA 2223521 A | 30-01-1997 |
| | | DE 69608108 D | 08-06-2000 |
| | | EP 0838123 A | 29-04-1998 |
| | | US 5966650 A | 12-10-1999 |
| WO 9631043 A | 03-10-1996 | AU 690441 B | 23-04-1998 |
| | | AU 5156396 A | 16-10-1996 |
| | | CA 2215361 A | 03-10-1996 |
| | | EP 0818103 A | 14-01-1998 |
| | | JP 11502982 T | 09-03-1999 |
| | | NO 974511 A | 30-09-1997 |
| | | NZ 304388 A | 24-09-1998 |
| | | US 5907602 A | 25-05-1999 |
| WO 9905844 A | 04-02-1999 | AU 8349698 A | 16-02-1999 |
| | | EP 0997028 A | 03-05-2000 |
| US 5375244 A | 20-12-1994 | NONE | |